

25X1

~~SECRET~~ [REDACTED]

**NATIONAL FOREIGN INTELLIGENCE BOARD**

WASHINGTON, D.C. 20505

NFIB 5.1/98

31 May 1988

**MEMORANDUM FOR NATIONAL FOREIGN INTELLIGENCE BOARD PRINCIPALS**

FROM: Executive Secretary, NFIB

25X1 SUBJECT: Revision of DCID 1/16 [REDACTED]

1. The Deputy Director of Central Intelligence has given preliminary approval to the attached draft revision of Director of Central Intelligence Directive (DCID) 1/16, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks, and requests that it be formally coordinated with you prior to promulgation by the DCI. The proposed revision was developed by an interagency working group sponsored by the DCI's Intelligence Information Handling Committee and Security Forum. A summary of its salient features and of related issues brought to the attention of the DDCI are provided in the Director, Intelligence Community Staff's forwarding memorandum appended for your information.

25X1

2. Your response by 15 June 1988 is requested.

25X1

[REDACTED]  
Mark J. Sullivan, Jr.

Attachments: As Stated

25X1

25X1

~~SECRET~~ [REDACTED]

SECRET

25X1

ICS 4046-88

29 April 1988

MEMORANDUM TO: Deputy Director of Central Intelligence

FROM: Lieutenant General Edward J. Heinz, USAF  
Director, Intelligence Community Staff

25X1

SUBJECT: Request for Review and Approval of Revised DCID 1/16

25X1

1. Actions Requested: (1) Your review of the attached draft revision of DCID 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks"; (2) your determination on the policy issue outlined in Attachment B; and (3) your decision as to whether to forward the draft DCID to NFIB Principals for formal coordination.

2. Background: An interagency working group, sponsored by the Information Handling Committee and the DCI's Security Forum, undertook a thorough review of DCID 1/16 and has drafted a substantial revision of that Directive and the guidance contained therein. There has been little substantive change to DCID 1/16 since it was originally promulgated in the early-1970s, and the policy guidance it provides has become badly outdated by changes in technology and security procedures. This has led to wide variations in security practice and procedure for protecting intelligence among Community components. The revised policy seeks to balance operational requirements, particularly those of DoD, and achievable security objectives, both technical and procedural. Much of the revised policy focuses on reducing known vulnerabilities of existing systems, in particular the thirteen "Critical Systems" identified by the DCI's COMPUSEC project. The principal features of the proposed policy guidance revision are outlined as follows:

- systems operating on multiple security levels are authorized under narrowly specified conditions;
- system accreditation requirements are tightened; multilevel systems must be accredited by the DCI, DIRNSA or D/DIA personally;

25X1

SECRET

SECRET

25X1

25X1 SUBJECT: Request for Review and Approval of Revised DCID 1/16

- DoD standards for evaluating the technical security features of an automated system are adopted to provide consistency across the Intelligence Community;
- provision is made for phased implementation of systems using "trusted products" evaluated by the National Computer Security Center;
- security guidance concerning networks has been clarified and expanded; and
- provision is made for incident reporting to better assess threats to and vulnerabilities of systems processing intelligence.

25X1

3. A universal matter of concern among the organizations which drafted the DCID revision is the potential resource impact of its implementation. Inasmuch as the proposed computer security guidance is both conceptually different from and more demanding than current requirements, particularly regarding security oversight of system configuration and operations throughout the system's life cycle, its proper application will require significantly greater staff effort. Resource impacts will likely correlate with the numbers of systems in the Community. Potentially, the DCID will impact almost all systems development and maintenance areas including: costs of hardware and software, storage requirements, throughput changes, administrative overhead, reallocation of people, training costs, and productivity. Given current fiscal constraints, it is not clear that the additional resources required will be available.

25X1

4. Furthermore, the combined impact of key conceptual changes (e.g., the addition of indirect users and their impact on both system boundaries and on the revised definitions of authorized system security modes) has an expected substantial, but not yet quantified, impact on collective accreditation requirements. For example, the revised DCID clarifies the definitions of the modes of operation and specifies that all people who receive output from an AIS, without reliable human review, must be considered in determining the mode of operation of the system. In the past, DoD (less NSA), but including Federal Department/Agency contractors under the DoD Industrial Security Program has not included in implementing policies, for mode determination, a consideration of indirect users who are electronically connected to a system. The new DCID requires that all electronically connected users (both directly and indirectly connected) be considered in determining the mode of operation and associated security requirements for accreditation. DIA and the Military Departments are concerned that this will raise the security and resource requirements for systems that are now in operation.

25X1

2

SECRET

25X1

SECRET

25X1

25X1

SUBJECT: Request for Review and Approval of Revised DCID 1/16

25X1

5. DIA's DCID 1/16 implementing policy and program has been limited in scope to those automated systems in DoD that process SCI. Within DoD, computer systems processing intelligence other than SCI are accredited under the SECDEF's AIS security implementation of 12356 in DoD Directive 5200.28. The revised DCID 1/16 clarifies the scope of systems covered to include all those that process intelligence under the DCI's statutory authority and responsibilities (e.g., including CIA DDO reporting, which is not SCI). DIA says that this change will result in significant additional resource expenditure.

25X1

6. Nonetheless, it is the view of participating agencies that the necessary security policy and procedures be established as the basis for planning and administrative action. Compliance dates established by the revised DCID have been adjusted to reflect anticipated resource constraints.

25X1

7. Community Coordination: All Community agencies, as well as OSD(P), ASD (C<sup>3</sup>I), and the National Computer Security Center, actively participated in the revision drafting process. Late drafts, including the attached, were formally coordinated with Community agencies through both the IHC and the DCI Security Forum. Although more than 50 issues were identified at the outset, only one could not be resolved and is submitted in Attachment B for your policy determination.

25X1

8. Recommendations: The organizations which participated in the drafting and review of the proposed DCID 1/16 revision believe it will be of substantial benefit to the Community's computer security program. Therefore, it is recommended that you approve it pending formal coordination by the NFIB. With regard to the policy question discussed in Attachment B, I recommend you approve Alternative D, but with the amendment proposed by C/IHC to make explicit a right of appeal to the DCI/DDCI. I support his view that the DCID should provide a mechanism for resolving impasses between data users and owners created by differing perceptions of the relative risk to sources and methods inherent in a given circumstance.

Edward J. Heinz  
Lieutenant General, USAF

## Attachments:

- A. DCID 1/16
- B. Decision Paper
  - Annex I, CIA Memo re Foreign Access
  - Annex II, NSA Memo re Foreign Access

3  
SECRET

25X1

SECRET

25X1

25X1 SUBJECT: Request for Review and Approval of Revised DCID 1/16

Forward Draft to NFIB for Formal Coordination:

25X1

APPROVED:

Deputy [Director for] Central Intelligence

5-17-88  
Date

DISAPPROVED:

Deputy Director for Central Intelligence Date

- - - - -

Foreign National Access to Community AIS:

APPROVE ALTERNATIVE A:

Deputy Director for Central Intelligence Date

APPROVE ALTERNATIVE B:

Deputy Director for Central Intelligence Date

APPROVE ALTERNATIVE C:

Deputy Director for Central Intelligence Date

APPROVE ALTERNATIVE D:

Deputy Director for Central Intelligence Date

25X1

APPROVE ALTERNATIVE D  
WITH C/IHC AMENDMENT

Deputy [Director for] Central Intelligence

5-17-88  
Date

DISAPPROVE ALL ALTERNATIVES:

Deputy Director for Central Intelligence Date

4

SECRET

25X1

**Page Denied**

Next 8 Page(s) In Document Denied



**NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
FORT GEORGE G. MEADE, MARYLAND 20755-6000**

Serial: T1-016L-88  
04 April 1988

**MEMORANDUM FOR THE CHAIRMAN, DIRECTOR OF CENTRAL INTELLIGENCE -  
INTELLIGENCE INFORMATION HANDLING COMMITTEE (IHC)**

**SUBJECT: DCID-16 - Proposal DDCI Decision Paper on  
Notification/Approval for Foreign National Access**

(FOUO) Based on further internal review and evaluation, NSA supports Alternative D. This position is based on concern for the protection of Signals Intelligence (SIGINT) processed and stored in a myriad of national and tactical systems being fielded by intelligence entities that receive, store and process SIGINT in its original form or in modified but classified form (sanitized or decompartmented). This concern extends to those indirect connections that constitute one-way electrical connections. Alternative D is also supported because it requires data owner concurrence vice consultation and thus preserves for the report originator a key role in risk assessment. A primary issue is assurance that the proposed policy not adversely affect existing responsibilities and authorities pertaining to information protection and release.

STAT



**NSA Member  
Intelligence Information  
Handling Committee**

**FOR OFFICIAL USE ONLY**